Proposed Language for FSA Contractual Agreements

1. Contractual Agreements

Arrangements involving outsourcing the development, operation, or testing of organizational information processing operations or facilities should be based on a formal contract containing, or referring to, all the security requirements needed to ensure compliance with the organization's security policies and standards. The contract should ensure that there is no misunderstanding between the organization and the third party.

Objectives:

- To maintain the security of information when the responsibility for information processing has been outsourced to another organization.
- Outsourcing arrangements should address the risks, security controls and security procedures for information systems, networks and/or desktop environments in the contract between the parties.

2. Rules and Regulations

FSA systems must adhere to the Federal security requirements detailed in both the Statement of Work of this contract and in the publications listed below. The following laws, regulations or policies establish requirements for confidentiality, integrity and availability for FSA contracts.

2.1. Federal Laws and Regulations

- Computer Security Act of 1987, Public Law 100-235, 101 Stat. 1724.
- Electronic Communications Privacy Act of 1986, Public Law 99-08, 100 Stat. 1848
- E-Government Act of 2002

- Fraud and Related Activity in Connection with Access Devices and Computers, 5 United States Code 1029-1030,
- Freedom of Information Act, 5 United States Code 552, Public Law 93-502
- Privacy Act of 1974, 5 United States Code 552a, Public Law 99-08
- Federal Information Security Management Act (FISMA)
- OMB Circulars A-123, A-127, A-130 Appendix III
- National Telecommunications Information System and Security Policy No. 2
- PDD 63 Critical Infrastructure Protection, May 1998

2.2. NIST Special Publications

- NIST 800-26 (Security Self-Assessment Guide for Information Technology Systems)
- NIST 800-18 (Guide for Developing Security Plans for Information Technology Systems)
- NIST 800-30 (Risk Management Guide)
- NIST 800-37 (Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems)
- NIST 800-47 (Security Guide for Interconnecting Information Technology Systems)
- NIST 800-16 (Information Technology Security Training Requirements: A Role and Performance-Based Model)
- NIST 800-14 (Generally Accepted Principles and Practices for Securing Information Technology Systems)
- NIST 800-12 (An Introduction to Computer Security: The NIST Handbook)

2.3. Departmental of Education Policies and Procedures

- U.S. Department of Education Information Technology Security Policy, Draft, February 2002
- U.S. Department of Education, Information Technology Security Manual, Handbook Number 6
- U.S. Department of Education, Personnel Security-Suitability Program, Handbook Number 11
- FSA Security Policy, April 2003
- FSA System Security Process Guide, March 2003
- New Department/ FSA security policies and procedures.

The Contractor may arrange to review copies of the above referenced documents by contracting the Contract Specialist at telephone number _____. The Contractor shall include this provision in any subcontract(s) awarded pursuant to this contract.

3. Security requirements in outsourced and third-party contracts

FSA's security requirements for outsourcing the management and control of any of its information technology assets and/or operations should be addressed in a contract agreed upon between the parties.

Contracts between FSA and outsourced/third parties should require that the contractor and all other outsourced/third parties (sub-contractors) must:

a) Follow Department of Education and Federal Student Aid general policy on information security;
b) Ensure all parties involved in the outsourcing, including subcontractors, are aware of their security and privacy responsibilities;
c) Participate in specialized security training at least annually;
d) Explain how the availability, integrity and confidentiality of the organization's business assets will be maintained and tested;
e) Determine what physical and logical controls will be used to restrict and limit the access to the organization's sensitive business information to authorized users;
f) Explain how the availability of services is to be maintained in the event of a disaster;
g) Describe the levels of physical security to be provided for outsourced equipment;
h) Allow the right of audit;
i) Include a description of each service to be made available;
j) Determine the respective liabilities of the parties to the agreement;
k) Establish an escalation process for problem resolution; contingency arrangements should also be considered where appropriate;
l) Establish a clear reporting structure and agreed reporting formats;
m) Establish a clear and specified process of change and configuration management;
n) Make arrangements for reporting, investigation, and resolution of security incidents and security breaches;
o) Document any involvement of the outsourced provider with relevant subcontractors.
p) Create required security documentation, including, but not limited to, System Security Plan, Risk Assessment, System Security Authorization Agreement (product from Certification and Accreditation), Rules of Behavior, MOUs and Contingency Planning documentation.

Although outsourcing contracts can pose some complex security questions, the controls included in this code of practice could serve as a starting point for agreeing the structure and content of the system security plan.

4. Personnel Security Requirements

The contractor agrees to comply with all Department of Education and FSA contractor clearance requirements, as defined in the Departmental regulations listed above. The contractor agrees to submit the appropriate screening information (fingerprints, etc) on all contractor staff immediately upon each staff person beginning work on the contract, or before, if deemed necessary by the Department. The contractor must notify FSA if an

individual's duties change within the scope of the contract or an individual departs the contract.

5. FSA Guidance for System Development Initiatives

Contractors must follow the FSA System Security Process Guide to make sure that security is an integral component of all FSA systems. The guide includes numerous aides to let a project team develop the security artifacts that will support the system's overall security posture and auditability. As the system progresses through the lifecycle, the project team must produce documents such as a system security plan and, for certification and accreditation, a security test and evaluation plan. The guide also provides direction for security training requirements, contingency planning, risk assessments, and other important security artifacts and activities. Security documents must be updated commensurate to system change. Use of the methodology established within this guide is a requirement for all new and revised systems, and should be incorporated within a projects scheduling.

6. Withholding of Contract Payments

Notwithstanding any other payment provisions of this contract, failure of the contractor to submit required forms, responses or reports when due; failure to perform or deliver required work, supplies, or services; or, failure to meet any of the requirements of the contract, to include all requirements as specified in Clause 307-13 Department Security Requirements (April 1999), will result in the withholding of payments under this contract in such amounts as the contracting officer deems appropriate, unless the failure arises out of causes beyond the control, and without the fault of negligence, of the contractor, as defined by the clause entitled 'Excusable Delays' or Default', as applicable. The Government shall promptly notify the contractor of its intention to withhold payment of any invoice or voucher submitted. Payment will be withheld until the failure is cured, a new delivery schedule is agreed upon, or payment is made as part of a termination settlement.

Should damage occur to Department assets, or additional costs be incurred as a direct result of contractor inaction, improper conduct in relation to security policy and practices, or failure to implement any of the Department's security policies and practices, the contractor will bear all related costs to correct the damage or deficiencies.